PERKINS COIE LLP
Susan D. Fahringer (Bar No. 162978)
SFahringer@perkinscoie.com
Nicola Menaldo (*Pro Hac Vice* Forthcoming)
NMenaldo@perkinscoie.com
Lauren J. Tsuji (Bar No. 300155)
LTsuji@perkinscoie.com
1201 Third Avenue, Suite 4900
Seattle, Washington 98101-3099
Telephone: 206.359.8000
Facsimile: 206.359.9000

Sunita Bali (Bar No. 274108)
SBali@perkinscoie.com
505 Howard Street, Suite 1000
San Francisco, California 94105-3204
Telephone: 415.344.7000
Facsimile: 415.344.7050

Attorneys for Defendants YouTube, LLC and Google LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

BRAD MARSCHKE, individually, and on behalf of all others similarly situated,

Plaintiff

v.

YOUTUBE, LLC and GOOGLE LLC,

Defendants.

Case No. 3:22-cv-06987-JD

DEFENDANTS' NOTICE OF MOTION AND MOTION TO DISMISS CLASS ACTION COMPLAINT

Date: February 16, 2023
Time: 10:00 a.m.
Location: Courtroom 11, 19th Floor
Judge: Hon. James Donato

NOTICE OF MOTION AND MOTION TO DISMISS

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that on February 16, 2023, at 10:00 a.m. or as soon thereafter as this Motion may be heard in the above-entitled court, located at 450 Golden Gate Avenue, San Francisco, California, in Courtroom 11, 19th Floor, Defendants YouTube, LLC and Google LLC, by and through their counsel of record, will and hereby do, move this Court for an order dismissing Plaintiff's Class Action Complaint (Dkt. No. 1) under Rule 12(b)(6) of the Federal Rules of Civil Procedure.

This Motion is based on this Notice of Motion and Motion, the Memorandum of Points and Authorities herein, the Request for Judicial Notice, the Declaration of Susan D. Fahringer in Support of Defendants' Motion to Dismiss Class Action Complaint and the exhibits attached thereto, the pleadings and papers on file in this action and all related cases, any argument and evidence to be presented at the hearing on this Motion, and any other matters that may properly come before the Court.

STATEMENT OF ISSUES

1. Whether Plaintiff has failed to allege facts showing that the data at issue qualifies as a "biometric identifier" or "biometric information" within the meaning of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1 *et seq.* ("BIPA").

2. Whether Plaintiff has failed to allege conduct that occurred primarily and substantially in Illinois, such that his claims would violate the prohibition against applying BIPA extraterritorially and the U.S. Constitution's dormant Commerce Clause.

3. Whether Plaintiff has failed to allege facts showing that he is "aggrieved" by any alleged violation of BIPA Section 15(a).

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

OTHER AUTHORITIES

MOTION TO DISMISS CLASS ACTION COMPLAINT

I. INTRODUCTION

This class action lawsuit targets two useful and important video editing tools made available on YouTube: (1) "Face Blur," a privacy-protective tool that allows a person who uploads a video to YouTube to blur specific faces and thereby protect the anonymity of bystanders, activists, and others who appear in the video, and (2) "Thumbnail Generator," a tool that allows the uploader to select a static image from the video to use as a preview or "thumbnail" of the video. Claiming that these tools violate the Illinois Biometric Information Privacy Act, 740 ILCS 14/1 *et seq.* ("BIPA"), Plaintiff Brad Marschke ("Marschke") seeks extraordinary statutory damages from YouTube, LLC and Google LLC ("Defendants"), as well as injunctive and other relief. But the Complaint does not come close to alleging facts sufficient to state a claim under BIPA, and it should be dismissed for at least the following reasons.

First, BIPA regulates the treatment of "biometric *identifier[s]*," which include "scan[s] of . . . face geometry," and information that is "based on" a biometric identifier and "used to *identify* an individual." *Id.* § 10 (emphasis added). But Marschke does not allege that the data at issue in this case identified him (or anyone else), and interpreting the statute to extend to the type of privacy-protective features at issue here would strain the ordinary meaning and contravene the purposes of BIPA.

Second, BIPA does not apply extraterritorially, but Marschke has not alleged that any of the conduct relevant to his claims occurred in Illinois. Applying BIPA to the facts alleged here would extend the statute beyond what the Illinois General Assembly intended and what Illinois law permits, and would raise serious constitutional concerns that this Court has a duty to avoid.

Third, Marschke is not "aggrieved" by Defendants' alleged failure to publish a biometric data retention policy, but "aggrievement" is an essential element of his Section 15(a) claim. His Section 15(a) claim should be dismissed for this additional and independent reason.

II. BACKGROUND

A. The Illinois Biometric Information Privacy Act

BIPA applies only to "biometric identifiers" and "biometric information." "Biometric identifier means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." BIPA § 14/10. "Biometric information means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." *Id.* Here, Marschke asserts claims for violation of BIPA Sections 14/15(a) and (b). Section 14/15(a) requires that a private entity "in possession" of covered data must "develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying" the data within certain timeframes. *Id.* § 15(a). Section 14/15(b) provides that a private entity may not "collect, capture, purchase, receive through trade, or otherwise obtain" (hereinafter "Collect") covered data unless it first obtains a "written release" (defined as "informed written consent," *id.* § 10) from the subject or the subject's "legally authorized representative." *Id.* § 15(b). "Any person aggrieved" by a violation of BIPA may sue for actual damages or liquidated damages of $1,000 per negligent violation or $5,000 per "intentional[]" or reckless[]" violation, as well as attorneys' fees and costs. *Id.* § 20.

B. Marschke's Allegations

Marschke's claims are based on his alleged use of the video-sharing platform YouTube. He targets two features made available to video creators through YouTube Studio: Face Blur, which allows video creators to blur certain faces wherever they appear in a video, and Thumbnail Generator, which allows video creators to select a specific image to use as a "thumbnail" or preview for the video. *See* Dkt. No. 1 ("Complaint" or "Compl.") ¶¶ 11–13. Marschke alleges that he has "uploaded multiple videos to his YouTube account that include images of his face," and has used both the Face Blur and Thumbnail Generator features on videos containing images of his face. *Id.* ¶ 72–74.

Marschke alleges that the Face Blur feature "relies on state-of-the-art facial recognition technology to scan videos, locate human faces, and create and store scans of face geometry." *Id.* ¶ 48. When a video creator applies the tool, Defendants allegedly "scan the entire video to detect

all unique faces within the video," "display all detected faces within the video and allow the creator to select which faces the creator would like to blur out," and "blur out the selected face throughout the duration" of the video. *Id.* ¶¶ 50-52. According to Marschke, "Defendants capture and store on their servers scans of face geometry from all detected faces[.]" *Id.* ¶ 53.

Marschke alleges that the Thumbnail Generator tool "auto-generates photographic thumbnails" *i.e.*, "screenshots from an uploaded video[.]" *Id.* ¶ 61. He speculates—on "information and belief"—that "Defendants scan all videos uploaded to YouTube for faces at the time the videos are uploaded, and then use this face data to auto-generate thumbnails that contain faces, and especially faces with more expression." *Id.* ¶ 63. Marschke does not allege that he suffered any harm as a result of Defendants' actions. Instead, he asserts that he need not allege any harm other than a technical violation of BIPA. *Id.* ¶ 79 n.24.

Marschke's two claims, for violation of Sections 15(a) and 15(b) of BIPA, expressly regard only biometric *identifiers*, not biometric information. *Id.* ¶¶ 91–92, 98. He seeks to bring these claims on behalf of himself and a sweeping class of "[a]ll residents of the State of Illinois who had their faceprints or face templates collected, captured, received, or otherwise obtained by Defendants through YouTube." *Id.* ¶ 80. The Complaint makes clear that Marschke considers this putative class to include *every Illinois resident whose face has appeared in a YouTube video*. *See, e.g.*, *id.* ¶ 67.

III. ARGUMENT

A. Legal Standard

A Rule 12(b)(6) motion tests the legal adequacy of a complaint. "Dismissal can be based on the lack of a cognizable legal theory or the absence of sufficient facts alleged under a cognizable legal theory." *Balistreri v. Pacifica Police Dep't*, 901 F.2d 696, 699 (9th Cir. 1988). To survive a motion to dismiss, "a complaint must contain sufficient factual matter, accepted as true, 'to state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "A pleading that offers 'labels and conclusions' or 'a formulaic recitation of the elements of a cause of action will not do.'" *Id.*

B. Marschke's Claims Fail Because He Has Not Alleged Facts Showing That the Data at Issue Qualify as Biometric Identifiers or Biometric Information.

Marschke's claims target features that do nothing more than distinguish the shapes of faces from one another. He does not allege that any of the faces are identified or known to Defendants (or even to Marschke himself—except for his own face). He does not allege, for example, that Defendants link the unknown faces in videos to identities, or that Defendants maintain a database that would allow them to do so. That he has not offered any such allegations is unsurprising, because the Face Blur feature that he targets is designed to *prevent* identification of people in videos, to enhance "visual anonymity" and to allow "people to share personal footage more widely and to speak out when they otherwise may not." *See* Declaration of Susan D. Fahringer in Support of Defendants' Motion to Dismiss ("Fahringer Decl."), Ex. A (Amanda Conway, *Face Blurring: When Footage Requires Anonymity*, YouTube Blog (July 18, 2012)) ("Whether you want to share sensitive protest footage without exposing the faces of the activists involved, or share the winning point in your 8-year-old's basketball game without broadcasting the children's faces to the world, our face blurring technology is a first step towards providing visual anonymity for video on YouTube.").[1]

BIPA applies only to biometric "identifiers" and biometric information "used to identify" a person. BIPA § 14/10. Because Marschke has not alleged facts showing that the data at issue in this case identify anyone, he has not alleged that Defendants Collected data covered by the statute. This failure is fatal to his claims.

1. To qualify as a "biometric identifier," data must identify a person.

A biometric "identifier" must identify a person. "A statute should be construed so that no word or phrase is rendered superfluous or meaningless." *See, e.g.*, *Kraft, Inc. v. Edgar*, 561 N.E.2d 656, 661 (Ill. 1990). In construing a statute, words must be given their plain and ordinary meaning. *See, e.g.*, *Murray v. Chi. Youth Ctr.*, 864 N.E.2d 176, 189 (Ill. 2007); *Connell v. Lima Corp.*, 988

[1] *See also, e.g.*, Fahringer Decl., Ex. B (Josh Halliday, *Google Introduces Face-Blurring to Protect Protesters on YouTube*, Guardian (July 19, 2012, 12:59 PM)), ("YouTube has become a popular destination for videos of protest and civil disobedience in many countries around the world. Activists involved in the Arab Spring uprising in the Middle East used the site as a way to share footage of unrest in the region.").

F.3d 1089, 1097 (9th Cir. 2021). The ordinary meaning of the word "identifier" is "one that identifies," i.e., "state[s] the identity of (someone or something)." *See Identifier*, Merriam-Webster, http://www.merriam-webster.com/dictionary/identifier (last accessed Nov. 21, 2022); *Identify*, Merriam-Webster, http://www.merriam-webster.com/dictionary/identify (last accessed Nov. 21, 2022); *Identify*, Black's Law Dictionary (11th ed. 2019) ("To prove the identity of (a person or thing)."). To qualify as a "biometric *identifier*," then, data must *identify* the subject, i.e., must consist of, or at least link to, identity information. To conclude otherwise would render the word "identifier" meaningless, which conflicts with well-established rules of statutory construction. *Kraft*, 561 N.E.2d at 661.

That BIPA only regulates identifying data is consistent with its stated purpose of protecting against the "heightened risk [of] identity theft" that may result if biometric data is compromised. BIPA § 5(c). To create a heightened risk of identity theft, data must be associated with an identity. And in interpreting the term "biometric identifier," courts have reached this very conclusion. *See, e.g.*, *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1094 (N.D. Ill. 2017) (interpreting "biometric identifier" to mean "a biology-based set of measurements . . . *that can be used to identify a person*") (emphasis added); *Carpenter v. McDonald's Corp.*, 580 F. Supp. 3d 512, 515 (N.D. Ill. 2022) ("[A] biometric identifier is a unique personal feature that *can be used to identify a person*.") (emphasis added).

Interpreting "biometric identifier" to require identity information is also consistent with the motivation for adopting BIPA. The impetus for the statute was the impending bankruptcy of Pay by Touch, a company that had installed fingerprint scanners in stores throughout Illinois to enable shoppers to pay for purchases using only their fingerprint. To associate a fingerprint with the right payment source, Pay by Touch maintained a database with identifying information. Pay by Touch's bankruptcy created a risk that it would sell this database, and the Illinois General Assembly reacted by enacting BIPA. *See* Fahringer Decl., Ex. C (IL H.R. Tran. 2008 Reg. Sess. No. 276, at 249 (May 30, 2008) (Statement of Rep. Kathleen A. Ryg)) (noting that Pay by Touch's bankruptcy "leaves thousands of customers . . . wondering what will become of their biometric and financial data"); *see also* Fahringer Decl., Ex. D (M.P. Dunleavey, *In the Blink of an Eye, You've Paid*, N.Y. Times

(Dec. 17, 2005)) ("Pay by Touch . . . developed systems that scan a consumer's fingerprint and link the scan to payment information."). This database is precisely the sort of information that poses the risks that the Illinois General Assembly sought to avoid, *because* it was capable of identifying the data subjects. The data at issue in this case is far different, does not pose the same risks, and is not covered by BIPA.

2. To qualify as "biometric information," data must be "used to identify" a person.

While biometric *identifiers* must themselves actually identify a person, biometric information must be (1) *based on* a biometric identifier and (2) actually *used* to identify. BIPA § 14/10. The "used to identify" limitation is necessary because without it, biometric information could include *any* information, so long as it was "based on" a biometric identifier. Using the example of Pay by Touch, information "based on" biometric identifiers could be interpreted to include data like dates and amounts for purchases made using the fingerprint scanning system, even if that information is aggregated (for example, reflected in company financial statements or reports). Further limiting "biometric information" to data that is "used to identify" a person at least brings the covered data closer to the biometric data that the Illinois General Assembly was concerned with regulating. *See Hubble v. Bi-State Dev. Agency of Ill.-Mo. Metro. Dist.*, 938 N.E.2d 483, 497 (Ill. 2010) ("A court construing the language of a statute will assume that the legislature did not intend to produce an absurd or unjust result, and will avoid a construction leading to an absurd result, if possible." (citations omitted)).

3. Marschke does not allege that the data at issue here "identify" or are "used to identify" anyone.

As to Face Blur, Marschke alleges merely that the feature "detect[s] all unique faces" in a video and captures "scans of face geometry from all detected faces[.]" Compl. ¶¶ 50–60. As to Thumbnail Generator, he alleges that the feature "detect[s] faces" in videos and assumes that it "scan[s], detect[s], and collect[s] facial geometry." *Id.* ¶¶ 61–67. Marschke's failure to allege any identifying activity is fatal to his claims, and readily distinguishes this case from others where courts have found the "identification" component of "biometric identifiers" and "biometric information" satisfied. For example, in *In re Facebook Biometric Information Privacy Litigation*,

185 F. Supp. 3d 1155 (N.D. Cal. 2016), the complaint alleged that when Facebook's "Tag Suggestions" feature "recognizes and identifies . . . faces appearing in [a] photograph, Facebook *will suggest that individual's name or automatically tag them*. In effect, the program *puts names on the faces in photos* . . . ." *Id.* at 1158 (emphasis added). Similarly, in *Monroy v. Shutterfly, Inc.*, No. 16 C 10984, 2017 WL 4099846 (N.D. Ill. Sept. 15, 2017), the complaint alleged that "whenever a new image is uploaded onto Shutterfly's site, the faces in the image are compared against those in the database" and "[i]f a face's geometry matches that of an individual already in its database, Shutterfly *suggests . . . the individual's name*." *Id.* at *1 (emphasis added). "If no match is found, Shutterfly *prompts the user to enter a name*." *Id.* (emphasis added). Here, in contrast, Marschke does not allege that either Face Blur or Thumbnail Generator "identifies" the people whose faces appear in videos—e.g., by linking a face with the subject's name or account—or even that the features are capable of doing so.

4. Extending BIPA to Face Blur and Thumbnail Generator would conflict with the purpose of BIPA.

A ruling that BIPA prohibits technology that merely distinguishes among images of faces without identifying anyone would have significant negative consequences that could not possibly have been intended by the Illinois General Assembly. *See e.g.*, *Vigil v. Take-Two Interactive Software, Inc.*, 235 F. Supp. 3d 499, 504 (S.D.N.Y. 2017) ("BIPA represents the Illinois legislature's judgment that the collection and storage of biometrics . . . is not in-of-itself undesirable or impermissible"), *aff'd in part, vacated and remanded in part on other grounds*, 717 F. App'x 12 (2d Cir. 2017). It would be impossible to locate and secure consent from everyone—users and non-users alike—whose face appears in a video on YouTube, yet that is what this suit seeks to require.[2] Marschke's interpretation of BIPA would effectively ban privacy protective features like face blurring, an absurd result that the Illinois General Assembly cannot possibly have intended. *See Hubble*, 938 N.E.2d at 497.

[2] Marschke's overbroad interpretation would require consent to be secured from *everyone*, not just Illinois residents, because whether someone is an Illinois resident could not be discerned based on an image of the person in a video.

This case is not unlike *Zellmer v. Facebook, Inc.*, No. 3:18-cv-01880-JD, 2022 WL 976981 (N.D. Cal. Mar. 31, 2022). In *Zellmer*, this Court was asked to consider whether BIPA should be construed to require a company to provide notice to and obtain consent from people who appear in photographs but whose identities are unknown—"non-users"—"who [are] for all practical purposes total strangers" to the company. *Id.* at *3. The Court observed that it would be "patently unreasonable to construe BIPA to mean that" companies are "required to provide notice to, and obtain consent from" such unknown people:

> [T]he Illinois legislature clearly contemplated that BIPA would apply [only] in situations where a business had at least some measure of knowing contact with and awareness of the people subject to biometric data collection.

Id. at *3–4. As the Court recognized, any other interpretation "would lead to obvious and insoluble problems," "put [companies] in an impossible position," and "impose extraordinary burdens on businesses," contrary to legislative intent. *Id.* at *4–5.

Marschke's claims suffer from this very defect. His putative class includes every Illinois resident whose face appears in a video uploaded to YouTube. *See* Compl. ¶¶ 80, 53. He does not allege that Defendants know (or even that Defendants *could* determine) the identities of the people whose faces appear in the videos. He does not even allege that Defendants know which faces, if any, are associated with account holders. He must do more than this to state a claim under BIPA. Because Marschke has not alleged facts showing that the data at issue identifies its subject or is used to do so, his claims should be dismissed.

C. Marschke's Claims Fail Because He Does Not Allege Conduct that Occurred Primarily and Substantially in Illinois.

Marschke does not allege that Defendants engaged in *any* conduct in Illinois, let alone conduct that violates BIPA. His claims therefore run afoul of the prohibition against applying the statute extraterritorially and the U.S. Constitution's dormant Commerce Clause, and should be dismissed for this independent reason.

1. Marschke's claims violate the extraterritoriality doctrine.

Every court to consider the issue agrees that BIPA has no extraterritorial effect, and that it regulates only conduct that occurs within the borders of Illinois. *See, e.g.*, *Vance v. Microsoft Corp.*,

No. C20-1082JLR, 2022 WL 9983979, at *6 (W.D. Wash. Oct. 17, 2022) ("Because BIPA does not contain such an express provision [authorizing extraterritorial effect], it does not apply extraterritorially to conduct outside of Illinois."); *McGoveran v. Amazon Web Servs., Inc.*, No. 20-cv-1399-LPS, 2021 WL 4502089, at *3 (D. Del. Sept. 30, 2021) ("BIPA violations must occur in Illinois in order for plaintiffs to obtain any relief."); *Rivera*, 238 F. Supp. 3d at 1100 (plaintiffs' "asserted violations of [BIPA] must have taken place in Illinois in order for them to win"). Conduct is deemed to occur in Illinois when "the circumstances that relate to the disputed transaction occur[red] *primarily and substantially* in Illinois." *Avery v. State Farm Mut. Auto. Ins.*, 835 N.E.2d 801, 854 (Ill. 2005) (emphasis added). This means that "the majority of circumstances relating to the alleged violation" must have occurred within the state. *Landau v. CNA Fin. Corp.*, 886 N.E.2d 405, 409 (Ill. App. 2008). There "is no single formula or bright-line test for determining whether a transaction occurs within [Illinois]." *Avery*, 835 N.E.2d at 854. Rather, "each case must be decided on its own facts." *Id.* Courts may consider a number of factors, including where an alleged scan of facial geometry occurred and where it was stored.[3] No single factor is dispositive, and the key question is whether the "bulk of the circumstances" giving rise to an alleged violation occurred "primarily and substantially" in Illinois. *Id.*; *Gros v. Midland Credit Mgmt.*, 525 F. Supp. 2d 1019, 1024 (N.D. Ill. 2007); *see also Vance*, 2022 WL 9983979, at *7–8 (holding that claims were barred by extraterritoriality doctrine as a matter of law, even where plaintiffs claimed that their biometric data was obtained from photos "taken and uploaded to the internet in Illinois" and stored on a server in Illinois, where defendant's conduct was "too attenuated and de minimis" to find that it occurred "primarily and substantially in Illinois").

Here, Marschke does not allege that *any* of the conduct he claims violates BIPA occurred in Illinois, let alone "primarily and substantially" in Illinois. *Avery*, 835 N.E.2d at 854. He alleges that Defendants "capture and store on their servers scans of face geometry" (Compl. ¶ 53; *see also*

[3] *See, e.g.*, *Monroy*, 2017 WL 4099846, at *6 (noting that "where the actual scan of . . . face geometry took place, and where the scan was stored once it was obtained" are "important circumstances" to consider with respect to extraterritoriality); *Rivera*, 238 F. Supp. 3d at 1102 (noting that "where . . . the alleged scans actually take place" is one of several factors to be considered).

id. ¶¶ 54, 67), but neither Defendant is based in Illinois. *Id.* ¶¶ 21–22. Marschke does not allege that Defendants have servers in Illinois, or that they Collect the data at issue in Illinois. The only connection Marschke makes to Illinois is his own residency. *Id.* ¶ 20. This is not enough. *See, e.g.*, *Walker v. S.W.I.F.T. SCRL*, 491 F. Supp. 2d 781, 795 (N.D. Ill. 2007) (dismissing claims as impermissibly extraterritorial where "the only connection to the state of Illinois is the fact that plaintiff . . . is a resident of Illinois"); *McGoveran*, 2021 WL 4502089, at *4 ("A plaintiff's residency is not enough to establish an Illinois connection in order to survive a motion to dismiss based on extraterritoriality.").

McGoveran is instructive. There, the plaintiffs were Illinois residents who alleged that their voices were recorded and analyzed by out-of-state defendants and that their "voiceprints" were stored on defendants' servers, which were not alleged to be located in Illinois. 2021 WL 4502089, at *2. The complaint's only alleged connection to Illinois was that the plaintiffs' phone calls "originated from Illinois," were "from Illinois citizens," and were placed from "clearly recognizable Illinois phone numbers." *Id.* at *4. Plaintiffs argued that defendants failed to satisfy BIPA's notice and consent requirements in Illinois, but the court rejected this argument, explaining that it "really makes no sense to assign a location for an act that did not occur," and, "[m]ore fundamentally, that argument depends on the assumption that [d]efendants were required to" comply with BIPA in Illinois, even though plaintiffs did not allege "any activity in Illinois that would impose such obligations on [d]efendants." *Id.* The court concluded that, "[s]imply put, there is no indication in the complaint that [d]efendants did anything in Illinois." *Id.* The Court held that the complaint alleged an improperly extraterritorial application of BIPA and dismissed the claims.[4]

The same reasoning applies here. Marschke does not, and cannot, allege that the data at issue—supposedly, scans of face geometry—was "created, possessed, or stored . . . in Illinois." *Id.* Instead, as in *McGoveran*, Marschke relies entirely on the mere fact of *his own* Illinois residency to argue that Defendants should be held liable under BIPA. *See, e.g.*, Compl. ¶ 20. This is

[4] The *McGoveran* court ultimately allowed plaintiffs' claims to proceed after the complaint was amended to add specific allegations that the defendants' conduct "occurred principally and substantially" in Illinois. *See* Case No. 20-1399-LPS, Dkt. 46 (D. Del. Feb. 14, 2022). Marschke makes no such allegations.

insufficient, and the Complaint is subject to dismissal for this reason, as well.[5]

2. Adopting Marschke's sweeping interpretation of BIPA would violate the U.S. Constitution's dormant Commerce Clause.

If BIPA were interpreted as Marschke urges, it would violate the U.S. Constitution's dormant Commerce Clause, a result this Court should avoid. *See, e.g.*, *Prison Legal News v. Ryan*, 39 F.4th 1121, 1131 (9th Cir. 2022) ("[W]here an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the statute to avoid such problems." (citation omitted)). The dormant Commerce Clause limits "the authority of the States to enact legislation affecting interstate commerce," and "precludes the application of a state statute" that has "the practical effect of . . . control[ling] conduct beyond the boundaries of the State," even where "the commerce has effects within the State." *Healy v. Beer Inst.*, 491 U.S. 324, 326 n.1, 336 (1989) (citations omitted); *see also Rivera*, 238 F. Supp. 3d at 1102–04 (considering arguments regarding dormant Commerce Clause "substantial"). For example, in *Sam Francis Foundation v. Christies, Inc.*, 784 F.3d 1320 (9th Cir. 2015) (en banc), the Ninth Circuit "easily conclude[d]" that a statute violated the dormant Commerce Clause where it sought to regulate out-of-state conduct with "no necessary connection with the state other than the residency" of those involved in the transaction. *Id.* at 1323. At issue in *Sam Francis* was a statute that required the seller of fine art to pay the artist a five percent royalty if "the seller resides in California or the sale takes place in California," even if the artwork was sold out-of-state or involved only out-of-state residents. *Id.* at 1322. The court held that the statute's royalty requirement violated the dormant Commerce Clause because it "facially regulate[d] a commercial transaction that 'takes place wholly outside of the State's borders.'" *Id.* at 1323–24 (citation omitted).

Here, Marschke asks the Court to interpret BIPA so that it sweeps just as broadly as the law invalidated in *Sam Francis*: Marschke asks this Court to impose BIPA's requirements on

[5] In *In re Facebook Biometric Information Privacy Litigation*, 326 F.R.D. 535 (N.D. Cal. 2018), *aff'd sub nom. Patel v. Facebook, Inc.*, 932 F.3d 1264 (9th Cir. 2019), this Court observed that there was no dispute that the case was "deeply rooted in Illinois," where "Facebook [had] not tendered any evidence to indicate that the circumstances relating to the challenged conduct did not occur 'primarily and substantially within' Illinois." *Id.* at 547 (citation omitted). There, Facebook's only argument as to extraterritoriality was based on its "assertion that its servers are not located within Illinois." *Id.* at 540, 547. Here, in contrast, the *only* alleged link to Illinois is Marschke's own residency.

Defendants' out-of-state conduct simply because he happens to reside in Illinois. The dormant Commerce Clause does not allow states to project their authority so broadly. *Healy*, 491 U.S. at 336; *see also, e.g.*, *McGoveran*, 2021 WL 4502089, at *6 (noting that it would be both "overly broad and ultimately untenable" to hold that BIPA applies whenever a plaintiff resides in Illinois because "if that rule were correct, then BIPA could impose liability on a vast number of corporations who do no business in Illinois and who lack any other significant connection to Illinois").

The dormant Commerce Clause also prevents "inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another State." *Healy*, 491 U.S. at 336–37. Applying BIPA to the facts alleged here would displace the regulatory regime of California, where Defendants are headquartered. *See* Compl. ¶¶ 21–22. Unlike Illinois, California does not broadly regulate Biometric Data. Even the California Consumer Privacy Act ("CCPA") and the California Privacy Rights Act ("CPRA"), Cal. Civ. Code § 1798.100 *et seq.*, do not require informed written consent for collection of biometric information (as does BIPA § 15(b)), or prohibit private entities from profiting from biometric information (as does BIPA § 15(c)), or provide any person who is "aggrieved" with a private right of action (as does BIPA § 20).[6] California has taken a different approach to the regulation of Biometric Data, and allowing Marschke's claims to proceed here would result in Illinois projecting its policy decisions into California. The dormant Commerce Clause forbids that result. The Court should reject Marschke's interpretation of the statute because it would render the statute unconstitutional. *See, e.g.*, *Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Constr. Trades Council*, 485 U.S. 568, 575 (1988) ("[W]here an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress."). Alternatively, if the Court does accept Marschke's interpretation of

[6] The CPRA does not require covered entities to provide notice or obtain consent for the collection of biometric data. Instead, the CPRA merely requires such entities to provide a mechanism for consumers to opt-out of sharing "sensitive personal information." Cal. Civ. Code § 1798.135. Even that requirement is limited to "[t]he processing of biometric information *for the purpose of uniquely identifying a consumer*." Cal. Civ. Code § 1798.140(b) (emphasis added).

BIPA, then it should find BIPA to be in violation of the dormant Commerce Clause and dismiss his claims on this basis.

D. Marschke Is Not "Aggrieved" By a Violation of Section 15(a).

Marschke's Section 15(a) claim also fails because he has not pleaded facts establishing that he is "aggrieved" by Defendants' alleged violation of that section, but only someone "aggrieved" by a violation may seek relief under BIPA. BIPA § 14/20. To be aggrieved, a plaintiff must "hav[e] legal rights that are adversely affected" or "invaded" by the defendant's conduct. *Rosenbach v. Six Flags Ent. Corp.*, 129 N.E.3d 1197, 1205 (Ill. 2019). To show he is aggrieved by a violation of Section 15(a), Marschke must plausibly allege facts showing that Defendants (1) violated a legal duty under Section 15(a), and (2) owed that legal duty to him specifically. *See, e.g.*, *Am. Sur. Co. v. Jones*, 51 N.E.2d 122, 125 (Ill. 1943) (appellants were not "aggrieved" because the action of which they complained "did not directly affect [their] interest"); *In re Facebook Biometric Info. Priv. Litig.*, 326 F.R.D. at 546 (holding that "a party is aggrieved" under BIPA "by an act that directly or immediately affects her legal interest"). BIPA's purpose and legislative history support this interpretation: BIPA's aim is to protect consumers' information, not to impose liability for violations that result in no actual harm. The legislature was concerned that the absence of "reasonable safeguards" would "discourage the proliferation" of biometrics-facilitated transactions. *Vigil*, 235 F. Supp. 3d at 504. It did not deem the use of biometrics "in-of-itself undesirable or impermissible." *Id.* Instead, BIPA targeted the misuse, not the safe use, of Biometric Data. *Id.* That BIPA aims to prevent specific, palpable harms (e.g., from disclosure or misuse) supports the view that only a person who suffers harm may seek relief under the statute.

Marschke cannot satisfy these requirements. Section 15(a) sets forth two requirements for entities in possession of Biometric Data: (1) to *develop* a BIPA-compliant policy and (2) to *comply with* that policy. BIPA § 15(a). Marschke alleges only a violation of the former. *See* Compl. ¶ 98. But this duty "is owed to the public generally, not to particular persons." *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 626 (7th Cir. 2020). To show he is "aggrieved" under Section 15(a), Marschke must allege facts showing that Defendants failed to *comply* with their policy as to *his* data—for example, that three years have passed since his last interaction with Defendants, but

Defendants have failed to destroy his Biometric Data. He has not done so. He has not shown that he is "aggrieved," and has not stated a claim for violation of Section 15(a).

IV. CONCLUSION

Marschke has not pleaded facts showing that the "Face Blur" and "Thumbnail Generator" features targeted by this case violate BIPA. Interpreting BIPA as Marschke urges would lead to absurd results and would render the statute unconstitutional. The Court should reject Marschke's arguments and dismiss the Complaint.

Dated: November 21, 2022

PERKINS COIE LLP

By: */s/ Susan D. Fahringer*
Susan D. Fahringer (Bar No. 162978)
Sunita Bali (Bar No. 274108)
Nicola Menaldo (*Pro Hac Vice* Forthcoming)
Lauren J. Tsuji (Bar No. 300155)

Attorneys for Defendants
YouTube, LLC and Google LLC